STIC Search Report-3/23/2006

```
Set     Items   Description
S1     666143   ENCRYPT??? OR SECUR??? OR RSA  OR PRIVATE OR PRIVACY OR CR-
             YPTOG?????? OR PGP OR SCRAMBL??? OR HASH??? OR PRETTY()GOOD()-
             PRIVACY OR DECRYPT??? OR ENCIPHER??? OR DECIPHER??? OR DECOD?-
             ?? OR VERIFY??? OR VERIFI?????? OR AUTHENTIC????? OR GATEKEEP-
             ???
S2        266   S1(100N)((FINITE OR GALOIS)()FIELD(3W)(POLYNOMIAL? ? OR AR-
             ITHMETIC? ?)  OR RIJNDAEL)
S3          0   S2(100N)(RADIX(3W)MULTIPLIER? ?)
S4          0   S2(100N)((FLEXIBL? OR DYNAMIC????)(10N)(ANTICIPAT??? OR SE-
             NS??? OR PREPAR?????)(10N)( MODULUS OR MODULO)(10N)( VALUE? ?
             OR NUMBER? ? OR RESULT? ? OR QUANTIT??? OR AMOUNT? ?))
S5         58   S2(100N)((PUBLIC OR PUBLISHED)()KEY? ? OR PKI)
S6         25   S5(100N)(ELLIPTIC()CURVE? ? OR ECC OR ECMQV OR ECDH OR ECI-
             ES OR ECDSA)
S7          0   S6 NOT (PD=(19990515:20020515) OR PD=(20020516:20050516) OR
              PD=(20050516:20060316))
S8          0   S5 NOT (PD=(19990515:20020515) OR PD=(20020516:20050516) OR
              PD=(20050516:20060316))
S9         43   S2(100N)(ELLIPTIC()CURVE? ? OR ECC OR ECMQV OR ECDH OR ECI-
             ES OR ECDSA)
S10         1   S9 NOT (PD=(19990515:20020515) OR PD=(20020516:20050516) OR
              PD=(20050516:20060316))
S11         0    (RADIX(3W)MULTIPLIER? ?)(100N)((FLEXIBL? OR DYNAMIC????)(1-
             0N)(ANTICIPAT??? OR SENS??? OR PREPAR?????)(10N)( MODULUS OR -
             MODULO)(10N)( VALUE? ? OR NUMBER? ? OR RESULT? ? OR QUANTIT???
              OR AMOUNT? ?))
S12         0    (RADIX(3W)MULTIPLIER? ?)(100N)((3 OR THREE)(3N)MULTIPLICAN-
             DS)
S13        21   RADIX(3W)MULTIPLIER? ? AND (S1 OR IC=(H04K OR H04L OR G09C
              OR G06F))
S14         5   S13 NOT (PD=(19990515:20020515) OR PD=(20020516:20050516) -
             OR PD=(20050516:20060316))
S15         4   AU=((DROR I? OR DROR, I?) AND (GRESSEL C? OR GRESSEL, C?) -
             AND (MOSTOVOY M? OR MOSTOVOY, M?) AND (MOLCHANOV A? OR MOLCHA-
             NOV, A?))
? show files
File 348:EUROPEAN PATENTS 1978-2006/MAR
File 349:PCT FULLTEXT 1979-2006/UB=20060309,UT=20060302
         (c) 2006 WIPO/Univentio
?
```

15/5/3   (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00855413   **Image available**
EXTENDING THE RANGE OF COMPUTATIONAL FIELDS OF INTEGERS
EXTENSION DU CHAMP D'APPLICATION COMPUTATIONNEL DES ENTIERS
Patent Applicant/Assignee:
  M-SYSTEMS FLASH DISK PIONEERS LTD, 3B Omer Industrial Park, 84965 Omer,

IL, IL (Residence), IL (Nationality), (For all designated states except: US)

Patent Applicant/Inventor:

DROR Itai , 13 Hartzit Street, 84965 Omer, IL, IL (Residence), IL (Nationality), (Designated only for: US)

GRESSEL Carmi David , Kibbutz Urim, 85530 Mobile Post Negev, IL, IL (Residence), IL (Nationality), (Designated only for: US)

MOSTOVOY Michael , 3 Michael Hazani Street, 84480 Beer Sheva, IL, IL (Residence), IL (Nationality), (Designated only for: US)

MOLCHANOV Alexey , 12 Jabotinsky Street, 84000 Beer Sheva, IL, IL (Residence), IL (Nationality), (Designated only for: US

Legal Representative:

COLB Sanford T Sanford T Colb & CO (et al) (agent), P.O. Box 2273, 76122 Rehovot, IL,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200189129 A2-A3 20011122 (WO 0189129)

Application: WO 2001IL425 20010514 (PCT/WO IL0100425)

Priority Application: IL 136151 20000515; IL 139674 20001114

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Main International Patent Class (v7): G06F-007/49

Publication Language: English

Filing Language: English

Fulltext Availability:

Detailed Description

Claims

Fulltext Word Count: 19125

English Abstract

An extension of serial (60)/parallel (50) Montgomery multiplication method (Figs. 1-2) with simultaneous reduction as previously implemented by the applicants, adapted innovatively to perform both in the prime number and in the GF(2"sup"q) polynomial based number field, in such a way as to simplify the flow of operands, by performing a multiple anticipatory function (430) to enhance the previous modular multiplication procedure.

French Abstract

L'invention concerne une extension de la methode de multiplication modulaire serie-parallele de Montgomery avec reduction simultanee, telle que mise en oeuvre anterieurement par les deposants, adaptee de facon novatrice pour se realiser tant dans le nombre premier que dans le domaine du nombre base sur le polynome GF(2"sup"q), ce qui permet de simplifier le flux d'operandes grace a une fonction anticipatoire multiple pouvant ameliorer les operations de multiplication modulaire anterieures.

Legal Status (Type, Date, Text)

Publication 20011122 A2 Without international search report and to be republished upon receipt of that report.
Search Rpt 20020328 Late publication of international search report
Republication 20020328 A3 With international search report.
Examination 20030103 Request for preliminary examination prior to end of 19th month from priority date

10/3,K/1 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00457881 **Image available**
ARITHMETIC PROCESSOR
PROCESSEUR ARITHMETIQUE
Patent Applicant/Assignee:
CERTICOM CORP,
VANSTONE Scott A,
LAMBERT Robert J,
GALLANT Robert,
JURISIC Aleksandar,
VADEKAR Ashok V,
Inventor(s):
VANSTONE Scott A,
LAMBERT Robert J,
GALLANT Robert,
JURISIC Aleksandar,
VADEKAR Ashok V,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9848345 A1 19981029
Application: WO 98CA467 19980420 (PCT/WO CA9800467)
Priority Application: GB 977861 19970418
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH HU
IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL
PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW GH GM KE LS
MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB
GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 7167

Fulltext Availability:
Detailed Description

Detailed Description
ARITHMETIC PROCESSOR
The present invention relates to a method and apparatus for performing **finite field** and integer **arithmetic** .

BACKGROUND OF THE INVENTION
Elliptic Curve (EC) **cryptography** over a **finite field** require **arithmetic**
operations of addition, multiplication, squaring and inversion.
Additionally, subtraction operations are also required if the...

...computing signatures, however these operations are required less

frequently than the finite field operations.

EC **cryptography** as an example, requires the full complement of modular and finite field operations, addition, subtraction, multiplication and inversion.

Field sizes for **cryptography** tend to be relatively large, requiring fast, 1 5 dedicated processors to perform the arithmetic...

```
?

Set     Items   Description
S1   10602105   ENCRYPT??? OR SECUR??? OR RSA  OR PRIVATE OR PRIVACY OR CR-
             YPTOG?????? OR PGP OR SCRAMBL??? OR HASH??? OR PRETTY()GOOD()-
             PRIVACY OR DECRYPT??? OR ENCIPHER??? OR DECIPHER??? OR DECOD?-
             ?? OR VERIFY??? OR VERIFI?????? OR AUTHENTIC????? OR GATEKEEP-
             ???
S2        670   S1(100N)((FINITE OR GALOIS)()FIELD(3W)(POLYNOMIAL? ? OR AR-
             ITHMETIC? ?)  OR RIJNDAEL)
S3          0   S2(100N)(RADIX(3W)MULTIPLIER? ?)
S4          0   S2(100N)((FLEXIBL? OR DYNAMIC????)(10N)(ANTICIPAT??? OR SE-
             NS??? OR PREPAR?????)(10N)( MODULUS OR MODULO)(10N)( VALUE? ?
             OR NUMBER? ? OR RESULT? ? OR QUANTIT??? OR AMOUNT? ?))
S5        142   S2(100N)((PUBLIC OR PUBLISHED)()KEY? ? OR PKI)
S6         19   S5(100N)(ELLIPTIC()CURVE? ? OR ECC OR ECMQV OR ECDH OR ECI-
             ES OR ECDSA)
S7          5   S6 AND (PY<2000 OR PD<19990515)
S8          7   (S5 AND (PY<2000 OR PD<19990515)) NOT S6
S9         10   RADIX(3W)MULTIPLIER? ?
S10         0   S9 AND (((FLEXIBL? OR DYNAMIC????)(10N)(ANTICIPAT??? OR SE-
             NS??? OR PREPAR?????)(10N)( MODULUS OR MODULO)(10N)( VALUE? ?
             OR NUMBER? ? OR RESULT? ? OR QUANTIT??? OR AMOUNT? ?)) OR ((3
             OR THREE OR THIRD)(3N)MULTIPLICAND? ?) OR MONTGOMERY)
S11        57   AU=((DROR I? OR DROR, I?) OR (GRESSEL C? OR GRESSEL, C?) OR
              (MOSTOVOY M? OR MOSTOVOY, M?) OR (MOLCHANOV A? OR MOLCHANOV,
             A?)) AND (PY<2000 OR PD<19990515)
S12         0   S11 AND ((FINITE OR GALOIS)()FIELD(3W)(POLYNOMIAL? ? OR AR-
             ITHMETIC? ?)  OR RIJNDAEL)
? show files
File 275:Gale Group Computer DB(TM) 1983-2006/Mar 15
         (c) 2006 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2006/Mar 15
         (c) 2006 The Gale group
File  16:Gale Group PROMT(R) 1990-2006/Mar 16
         (c) 2006 The Gale Group
File 624:McGraw-Hill Publications 1985-2006/Mar 16
         (c) 2006 McGraw-Hill Co. Inc
File 484:Periodical Abs Plustext 1986-2006/Mar W2
         (c) 2006 ProQuest
File 613:PR Newswire 1999-2006/Mar 16
         (c) 2006 PR Newswire Association Inc
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 239:Mathsci 1940-2006/Apr
         (c) 2006 American Mathematical Society
File 370:Science 1996-1999/Jul W3
         (c) 1999 AAAS
File 696:DIALOG Telecom. Newsletters 1995-2006/Mar 16
```

```
         (c) 2006 Dialog
File 621:Gale Group New Prod.Annou:(R) 1985-2006/Mar 15
         (c) 2006 The Gale Group
File 674:Computer News Fulltext 1989-2006/Mar W2
         (c) 2006 IDG Communications
File  88:Gale Group Business A.R.T.S. 1976-2006/Mar 09
         (c) 2006 The Gale Group
File 369:New Scientist 1994-2006/Aug W4
         (c) 2006 Reed Business Information Ltd.
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 635:Business Dateline(R) 1985-2006/Mar 16
         (c) 2006 ProQuest Info&Learning
File  15:ABI/Inform(R) 1971-2006/Mar 16
         (c) 2006 ProQuest Info&Learning
File   9:Business & Industry(R) Jul/1994-2006/Mar 15
         (c) 2006  The Gale Group
File  13:BAMP 2006/Mar W1
         (c) 2006  The Gale Group
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 610:Business Wire 1999-2006/Mar 16
         (c) 2006 Business Wire.
File 647:CMP  Computer Fulltext 1988-2006/Apr W1
         (c) 2006 CMP Media, LLC
File  98:General Sci Abs 1984-2004/Dec
         (c) 2005 The HW Wilson Co.
File 148:Gale Group Trade & Industry DB 1976-2006/Mar 15
         (c)2006 The Gale Group
File 634:San Jose Mercury  Jun 1985-2006/Mar 15
         (c) 2006 San Jose Mercury News
File 256:TecInfoSource 82-2006/Feb
         (c) 2006 Info.Sources Inc
?

Set     Items   Description
S1     2614979   ENCRYPT??? OR SECUR??? OR RSA  OR PRIVATE OR PRIVACY OR CR-
             YPTOG?????? OR PGP OR SCRAMBL??? OR HASH??? OR PRETTY()GOOD()-
             PRIVACY OR DECRYPT??? OR ENCIPHER??? OR DECIPHER??? OR DECOD?-
             ?? OR VERIFY??? OR VERIFI?????? OR AUTHENTIC????? OR GATEKEEP-
             ???
S2         908   S1 AND ((FINITE OR GALOIS)()FIELD(3W)(POLYNOMIAL? ? OR ARI-
             THMETIC? ?)  OR RIJNDAEL)
S3           1   S2 AND RADIX(3W)MULTIPLIER? ?
S4           0   S2 AND ((FLEXIBL? OR DYNAMIC????)(10N)(ANTICIPAT??? OR SEN-
             S??? OR PREPAR?????)(10N)( MODULUS OR MODULO)(10N)( VALUE? ? -
             OR NUMBER? ? OR RESULT? ? OR QUANTIT??? OR AMOUNT? ?))
S5         101   S2 AND ((PUBLIC OR PUBLISHED)()KEY? ? OR PKI)
S6          36   S5 AND (ELLIPTIC()CURVE? ? OR ECC OR ECMQV OR ECDH OR ECIES
              OR ECDSA)
S7           7   S6 AND (PY<2000 OR PD<19990515)
S8          14   (S5 AND (PY<2000 OR PD<19990515)) NOT S6
S9         180   RADIX(3W)MULTIPLIER? ?
S10         35   S9 AND (((FLEXIBL? OR DYNAMIC????)(10N)(ANTICIPAT??? OR SE-
             NS??? OR PREPAR?????)(10N)( MODULUS OR MODULO)(10N)( VALUE? ?
             OR NUMBER? ? OR RESULT? ? OR QUANTIT??? OR AMOUNT? ?)) OR ((3
             OR THREE OR THIRD)(3N)MULTIPLICAND? ?) OR MONTGOMERY)
```

```
S11        11   S10 AND (PY<2000 OR PD<19990515)
? show files
File   2:INSPEC 1898-2006/Mar W1
         (c) 2006 Institution of Electrical Engineers
File   6:NTIS 1964-2006/Mar W1
         (c) 2006 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2006/Mar W1
         (c) 2006 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2006/Mar W2
         (c) 2006 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2006/Feb
         (c) 2006 ProQuest Info&Learning
File  56:Computer and Information Systems Abstracts 1966-2006/Mar
         (c) 2006 CSA.
File  57:Electronics & Communications Abstracts 1966-2006/Feb
         (c) 2006 CSA.
File  60:ANTE: Abstracts in New Tech & Engineer 1966-2006/Mar
         (c) 2006 CSA.
File  65:Inside Conferences 1993-2006/Mar 16
         (c) 2006 BLDSC all rts. reserv.
File  94:JICST-EPlus 1985-2006/Dec W3
         (c)2006 Japan Science and Tech Corp(JST)
File  95:TEME-Technology & Management 1989-2006/Mar W2
         (c) 2006 FIZ TECHNIK
File  99:Wilson Appl. Sci & Tech Abs 1983-2006/Feb
         (c) 2006 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2006/Mar 08
         (c) 2006 The Gale Group
File 144:Pascal 1973-2006/Feb W3
         (c) 2006 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File 636:Gale Group Newsletter DB(TM) 1987-2006/Mar 15
         (c) 2006 The Gale Group
?
```

8/9/6   (Item 6 from file: 2)
DIALOG(R)File   2:INSPEC
(c) 2006 Institution of Electrical Engineers. All rts. reserv.

03034449   INSPEC Abstract Number: B83025940, C83015529
Title: A single-chip VLSI implementation of the discrete exponential public key distribution system
Author(s): Kai Yiu; Peterson, K.
Author Affiliation: Hewlett-Packard Labs., Palo Alto, CA, USA
Conference Title: GLOBECOM '82. IEEE Global Telecommunications Conference p.173-9 vol.1
Publisher: IEEE, New York, NY, USA
Publication Date: 1982 Country of Publication: USA 3 vol. xxi+1383 pp.
U.S. Copyright Clearance Center Code: CH1819-2/82-0000-0173$00.75
Conference Sponsor: IEEE
Conference Date: 29 Nov.-2 Dec. 1982 Conference Location: Miami, FL, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Applications (A); Practical (P)

Abstract: Describes a single chip **Public Key** Distribution System (PKDS) based on Hellman's discrete exponential algorithm and **Galois field arithmetic** . A single VLSI high-speed PKDS has been designed and implemented for the network environment. This system is configured to operate in a number system which resembles an extended Galois field, GF(2/sup m/). Linear feedback shift register is used to implement the arithmetic operations such as add, multiply, and module operations. Since there are no carry and borrow required for **Galois field arithmetic** , high-speed **public key** distribution/exchange becomes feasible. The hardware was implemented by CMOS logic and fits in a 5"*7" single card. Since the system architecture is simple and modular, it is quite suitable for VLSI implementation. The VLSI PKDS chip has been fabricated using a 3 micron NMOS process and is designed to support a 4 MHz clock rate. This chip is believed to bridge the gap between the classical theory of **cryptography** and the practical **encryption** applications. (16 Refs)

Subfile: B C

Descriptors: **cryptography** ; data communication systems; large scale integration

Identifiers: Hellman discrete exponential algorithm; linear feedback shift register; single-chip VLSI; **public key** distribution system; **Galois field arithmetic** ; number system; extended Galois field; arithmetic operations; add; multiply; module operations; CMOS logic; 3 micron NMOS process; 4 MHz clock rate; **cryptography** ; **encryption**

Class Codes: B2570D (CMOS integrated circuits); B6120B (Codes); B6210 (Telecommunication applications); C0230 (Economic, social and political aspects)

8/9/12 (Item 1 from file: 56)

DIALOG(R)File 56:Computer and Information Systems Abstracts

0000162576 IP ACCESSION NO: 1999124

Algorithm engineering for public key **algorithms.**

Beth, T; Gollmann, D

Fak. Inf., Univ. Karlsruhe, 7500 Karlsruhe 1, FRG

IEEE J. SELECTED AREAS COMMUN., v 7, n 4, p 458-466, **1989**

PUBLICATION DATE: **1989**

DOCUMENT TYPE: Journal Article

RECORD TYPE: Abstract

LANGUAGE: English

FILE SEGMENT: Computer & Information Systems Abstracts

ABSTRACT:

The authors will examine ways of implementing **public key** algorithms based on modular integer arithmetic (**RSA**) and **finite field arithmetic** (Diffie-Hellman, ElGamal). In particular, they will be concerned with architectures for VLSI implementations.

DESCRIPTORS: **Cryptography** ; **Encryption** ; Arithmetic; Very large scale integration

IDENTIFIERS: **security** ; algorithms

SUBJ CATG: C CG4, **SECURITY**

8/9/14 (Item 2 from file: 144)
DIALOG(R)File 144:Pascal

11321225 PASCAL No.: 94-0142385
Architectures for exponentiation over GF(2 SUP n) adopted for smartcard application
ARAZI B
Ben Gurion univ., dep. electrical computer eng., Beer Sheva 84105, Israel
Journal: IEEE transactions on computers, **1993** , 42 (4) 494-497
ISSN: 0018-9340 CODEN: ITCOB4 Availability: INIST-222 F4; 354000033918450100
No. of Refs.: 14 ref.
Document Type: P (Serial) ; A (Analytic)
Country of Publication: USA
Language: English
Two exponentiation circuits over GF(2 SUP n) are proposed. Using the fact that squaring is a linear operation over GF(2 SUP n), a time-space tradeoff in smartcard-based circuitry is presented. It is further shown how multiplication is performed by a single shift, based on replacing the **public key** alpha SUP alpha element of GF(2 SUP n) by its minimal polynomial. Other considerations, related to structure regularity and the possible use of dynamic shift registers, are also treated

English Descriptors: **Cryptography** ; VLSI circuit; Integrated circuit; **Finite field arithmetics** ; Galois field

French Descriptors: **Cryptographie** ; Circuit VLSI; Circuit integre; Arithmetique champ fini; Champ galois

Classification Codes: 001D03F06
?

7/9/7 (Item 1 from file: 144)
DIALOG(R)File 144:Pascal

13799177 PASCAL No.: 98-0513694
Optimal extension fields for fast arithmetic in public - key **algorithms**
CRYPTO '98 : advances in cryptology : Santa Barbara CA, 23-27 August 1998
BAILEY D V; PAAR C
KRAWCZYK Hugo, ed
Computer Science Department, Worcester Polytechnic Institute, Worcester, MA 01609, United States; ECE Department, Worcester Polytechnic Institute, Worcester, MA 01609, United States
International Association for Cryptologic Research, International.
Annual international cryptology conference, 18 (Santa Barbara CA USA) 1998-08-23
Journal: Lecture notes in computer science, **1998** , 1462 472-485
ISBN: 3-540-64892-5 ISSN: 0302-9743 Availability: INIST-16343; 354000070095180330
No. of Refs.: 19 ref.
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)
Country of Publication: Germany; United States
Language: English
This contribution introduces a class of Galois field used to achieve fast

finite field arithmetic which we call an Optimal Extension Field (OEF). This approach is well suited for implementation of **public - key** cryptosystems based on elliptic and hyperelliptic curves. Whereas previous reported optimizations focus on finite fields of the form GF(p) and GF(2 SUP m), an OEF is the class of fields GF(p SUP m), for p a prime of special form and m a positive integer. Modern RISC workstation processors are optimized to perform integer arithmetic on integers of size up to the word size of the processor. Our construction employs well-known techniques for fast **finite field arithmetic** which fully exploit the fast integer arithmetic found on these processors. In this paper, we describe our methods to perform the arithmetic in an OEF and the methods to construct OEFs. We provide a list of OEFs tailored for processors with 8, 16, 32, and 64 bit word sizes. We report on our application of this approach to construction of **elliptic curve** cryptosystems and demonstrate a substantial performance improvement over all previous reported software implementations of **Galois field arithmetic** for **elliptic curves** .

English Descriptors: **Cryptography** ; **Public key**

French Descriptors: **Cryptographie** ; Cle publique

Classification Codes: 001D04A04E

7/9/1 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

07662795 INSPEC Abstract Number: B2000-09-1265B-050, C2000-09-5120-014
Title: VLSI design of F(s/sup 2n/) multiplier for elliptic curves **cryptosystem**
Author(s): Sutikno, S.; Surya, A.
Author Affiliation: Dept. of Electr. Eng., Bandung Inst. of Technol., Indonesia
Conference Title: 1999 IEEE International Symposium on Intelligent Signal Processing and Communication Systems. Signal Processing and Communications Beyond 2000 p.319-22
Publisher: King Mongkuts Inst. Technol, Bangkok, Thailand
Publication Date: 1999 Country of Publication: Thailand xxvii+804 pp.
ISBN: 974 622 612 6 Material Identity Number: XX-1999-01375
Conference Title: Proceedings of the International Workshop on Intelligent Signal Processing and Communication Systems
Conference Sponsor: Nat. Sci. & Technol. Dev. Agency (NSTDA); Nat. Electron. & Comput. Technol. Center (NECTEC); Japan Int. Cooperation Agency (JICA); Sirindhorn Int. Inst. Technol. (SIIT), Thammasat Univ.; IEEE Commun. Soc
Conference Date: 8-10 Dec. 1999 Conference Location: Phuket, Thailand
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: An **elliptic curves** cryptosystem is a high performance **public key** cryptosystem. This cryptosystem offers higher **security** level, smaller key size, lower bandwith and higher efficiency compared with other **public key** cryptosystems. An implementation of the **elliptic curves** cryptosystem needs a high performance **finite field arithmetic** module. In this paper we discuss a VLSI architecture of a finite field

F(2/sup 2n/) multiplier using normal basis representations. Using the proposed architecture, we obtain a faster computational time and the lower complexity architecture compares with other architectures. (8 Refs)
Subfile: B C
Descriptors: computational complexity; multiplying circuits; **public key cryptography** ; VLSI
Identifiers: VLSI design; F(s/sup 2n/) multiplier; **elliptic curves** cryptosystem; high performance **public key** cryptosystem; **security** ; key size; bandwith; efficiency; **finite field arithmetic** module; normal basis representations; computational time; complexity
Class Codes: B1265B (Logic circuits); B6120D (Cryptography); C5120 (Logic and switching circuits); C6130S (Data security)

11/9/9 (Item 1 from file: 57)
DIALOG(R)File 57:Electronics & Communications Abstracts

0000165456 IP ACCESSION NO: 0247060
Hybrid radix-4/radix-8 low power, high speed multiplier architecture for wide bit widths

Cherkauer, Brian S; Friedman, Eby G
Intel Corp, Santa Clara, CA, USA

PROC IEEE INT SYMP CIRCUITS SYST, v 4, p 53-56, **1996**
PUBLICATION DATE: **1996**

PUBLISHER: IEEE, PISCATAWAY, NJ, (USA)

CONFERENCE:
The 1996 IEEE International Symposium on Circuits and Systems, ISCAS. Part 4 (of 4), Atlanta, GA, USA, 12-15 May 1996

DOCUMENT TYPE: Conference Paper; Journal Article
RECORD TYPE: Abstract
LANGUAGE: English
ISSN: 0271-4310
FILE SEGMENT: Electronics & Communications Abstracts

ABSTRACT:
A hybrid radix-4/radix-8 architecture targeted for high bit multipliers is presented as a compromise between the high speed of a **radix** -4 **multiplier** architecture and the low power dissipation of a **radix** -8 **multiplier** architecture. In this hybrid **radix** -4/ **radix** -8 **multiplier** architecture, the performance bottleneck of a **radix** -8 **multiplier** , the generation of **three** times the **multiplicand** for use in generating the radix-8 partial product, is performed in parallel with the reduction of the radix-4 partial products rather than serially, as in a **radix** -8 **multiplier** . This hybrid **radix** -4/ **radix** -8 **multiplier** architecture requires 13% less power for a 64 x 64 bit multiplier, and results in only a 9% increase in delay, as compared with a radix-4 implementation. When supply voltage is scaled such that all multipliers exhibit the same delay, the 64 x 64 bit hybrid **radix** -4/ **radix** -8 **multiplier** dissipates less power than either the radix-4 or **radix** -8 **multipliers** . The hybrid radix-4/radix-8 architecture is therefore appropriate for those

applications that must dissipate minimal power and operate at high speeds.

DESCRIPTORS: Hybrid integrated circuits; Performance; Parallel processing systems; Delay circuits; Carry logic; Adders; Electric losses; Counting circuits
IDENTIFIERS: Power dissipation; Carry save adders; Complementary pass transistor logic family
SUBJ CATG: E 721.3, Computer Circuits; E 714.2, Semiconductor Devices and Integrated Circuits; E 722.4, Digital Computers and Systems; E 721.2, Logic Elements; E 701.1, Electricity: Basic Concepts and Phenomena; E 713.4, Pulse Circuits

```
Set     Items   Description
S1     1048934   ENCRYPT??? OR SECUR??? OR RSA  OR PRIVATE OR PRIVACY OR CR-
             YPTOG?????? OR PGP OR SCRAMBL??? OR HASH??? OR PRETTY()GOOD()-
             PRIVACY OR DECRYPT??? OR ENCIPHER??? OR DECIPHER??? OR DECOD?-
             ?? OR VERIFY??? OR VERIFI?????? OR AUTHENTIC????? OR GATEKEEP-
             ???
S2          70   S1 AND ((FINITE OR GALOIS)()FIELD(3W)(POLYNOMIAL? ? OR ARI-
             THMETIC? ?)  OR RIJNDAEL)
S3           0   S2 AND RADIX(3W)MULTIPLIER? ?
S4           0   S2 AND ((FLEXIBL? OR DYNAMIC????)(10N)(ANTICIPAT??? OR SEN-
             S??? OR PREPAR?????)(10N)( MODULUS OR MODULO)(10N)( VALUE? ? -
             OR NUMBER? ? OR RESULT? ? OR QUANTIT??? OR AMOUNT? ?))
S5           0   S2 AND ((PUBLIC OR PUBLISHED)()KEY? ? OR PKI)
S6           3   S2 AND (ELLIPTIC()CURVE? ? OR ECC OR ECMQV OR ECDH OR ECIES
              OR ECDSA)
S7          42   S2 NOT (S6 OR AD=(1990515:20020515) OR AD=(20020515:200603-
             16))
S8          10   RADIX(3W)MULTIPLIER? ?
S9           1   S8 AND (((FLEXIBL? OR DYNAMIC????)(10N)(ANTICIPAT??? OR SE-
             NS??? OR PREPAR?????)(10N)( MODULUS OR MODULO)(10N)( VALUE? ?
             OR NUMBER? ? OR RESULT? ? OR QUANTIT??? OR AMOUNT? ?)) OR ((3
             OR THREE OR THIRD)(3N)MULTIPLICAND? ?) OR MONTGOMERY)
S10          8   ((RADIX(3W)MULTIPLIER? ?) AND IC=(H04K OR H04K OR G09C OR -
             G06F)) NOT S9
S11         68   (((FINITE OR GALOIS)()FIELD(3W)(POLYNOMIAL? ? OR ARITHMETI-
             C? ?)  OR RIJNDAEL) AND IC=(H04K OR H04K OR G09C OR G06F)) NOT
              (S6 OR AD=(1990515:20020515) OR AD=(20020515:20060316))
? show files
File 347:JAPIO Nov 1976-2005/Nov(Updated 060302)
         (c) 2006 JPO & JAPIO
File 350:Derwent WPIX 1963-2006/UD,UM &UP=200617
         (c) 2006  Thomson Derwent
?
```

6/5/3   (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012166956   **Image available**
WPI Acc No: 1998-583868/199849
XRPX Acc No: N98-454824
Arithmetic processor e.g. for performing finite field **and integer** arithmetic **- has arithmetic logic unit having several arithmetic circuits performing group of associated arithmetic operation with arithmetic logic unit having operand input data bus and result data**

output bus to return results of operation on it

Patent Assignee: CERTICOM CORP (CERT-N); VANSTONE S A (VANS-I); MOTOROLA INC (MOTI)

Inventor: GALLANT R; JURISIC A; LAMBERT R J; VADEKAR A V; VANSTONE S A; DWORKIN J D; GLASER P M; TORLA M J; VADEKAR A

Number of Countries: 081 Number of Patents: 013

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9848345	A1	19981029	WO 98CA467	A	19980420	199849	B
AU 9873291	A	19981113	AU 9873291	A	19980420	199913	
EP 976027	A1	20000202	EP 98920431	A	19980420	200011	
			WO 98CA467	A	19980420		
US 6230179	B1	20010508	US 97997960	A	19971224	200128	
US 6266717	B1	20010724	US 97997964	A	19971224	200146	
JP 2001520775	W	20011030	JP 98544618	A	19980420	200202	
			WO 98CA467	A	19980420		
US 6349318	B1	20020219	WO 98CA467	A	19980420	200221	
			US 99418217	A	19991014		
US 20020136402	A1	20020926	WO 98CA467	A	19980420	200265	
			US 99418217	A	19991014		
			US 200123934	A	20011221		
EP 976027	B1	20030305	EP 98920431	A	19980420	200318	
			WO 98CA467	A	19980420		
			EP 200227872	A	19980420		
EP 1293891	A2	20030319	EP 98920431	A	19980420	200322	
			EP 200227872	A	19980420		
DE 69811877	E	20030410	DE 98611877	A	19980420	200332	
			EP 98920431	A	19980420		
			WO 98CA467	A	19980420		
US 6735611	B2	20040511	WO 98CA467	A	19980420	200431	
			US 99418217	A	19991014		
			US 200123934	A	20011221		
US 20050044124	A1	20050224	WO 98CA467	A	19980420	200515	
			US 99418217	A	19991014		
			US 200123934	A	20011221		
			US 2004837749	A	20040504		

Priority Applications (No Type Date): GB 977861 A 19970418

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9848345	A1	E	37	G06F-007/72	

Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH HU IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
AU 9873291	A			G06F-007/72	Based on patent WO 9848345
EP 976027	A1	E		G06F-007/72	Based on patent WO 9848345

Designated States (Regional): CH DE FR GB LI

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6230179	B1			G06F-007/00	
US 6266717	B1			G06F-013/14	
JP 2001520775	W		37	G06F-007/72	Based on patent WO 9848345
US 6349318	B1			G06F-007/00	Cont of application WO 98CA467
US 20020136402	A1			H04L-009/00	Cont of application WO 98CA467 Div ex application US 99418217 Div ex patent US 6349318

```
EP 976027     B1 E     G06F-007/72   Related to application EP 200227872
                                     Based on patent WO 9848345
   Designated States (Regional): CH DE FR GB LI
EP 1293891    A2 E     G06F-007/72   Div ex application EP 98920431
                                     Div ex patent EP 976027
   Designated States (Regional): CH DE FR GB LI
DE 69811877   E        G06F-007/72   Based on patent EP 976027
                                     Based on patent WO 9848345
US 6735611    B2       G06F-007/00   Cont of application WO 98CA467
                                     Div ex application US 99418217
                                     Div ex patent US 6349318
US 20050044124 A1       G06F-007/00   Cont of application WO 98CA467
                                     Div ex application US 99418217
                                     Cont of application US 200123934
                                     Div ex patent US 6349318
                                     Cont of patent US 6735611
```

Abstract (Basic): WO 9848345 A

The processor comprises an arithmetic logic unit (ALU) having a **finite field arithmetic** circuit performing **finite field arithmetic** operations and a modular integer arithmetic circuit performing modular integer arithmetic operations. The arithmetic logic unit has an operand input data bus to receive operand data on it and a result data output bus which returns the results of the arithmetic operations on it. A register file is coupled to the operand data bus and the result data bus.

A controller is coupled to the ALU and the register file, the controller selects one of the finite field operations or the integer arithmetic operations in response to a mode control signal and controls data access between the register file and the ALU and so the register file is shared by both the finite filed and integer arithmetic circuits. The register file includes general-purpose registers and the ALU has a processing bit width greater than the operand buses data bit width. The controller is programmed with instructions to control a selected arithmetic operation of the arithmetic logic unit. The operand buses has a bit width the same as a processing bit width of the ALU and the result data bus bit width.

ADVANTAGE - Combines finite filed arithmetic and integer and provides operations required for **Elliptic Curve cryptography** and modular exponentiation for **RSA cryptography** .

Dwg.3/10

Title Terms: ARITHMETIC; PROCESSOR; PERFORMANCE; FINITE; FIELD; INTEGER; ARITHMETIC; ARITHMETIC; LOGIC; UNIT; ARITHMETIC; CIRCUIT; PERFORMANCE; GROUP; ASSOCIATE; ARITHMETIC; OPERATE; ARITHMETIC; LOGIC; UNIT; OPERAND; INPUT; DATA; BUS; RESULT; DATA; OUTPUT; BUS; RETURN; RESULT; OPERATE

Derwent Class: P85; T01

International Patent Class (Main): G06F-007/00; G06F-007/72; G06F-013/14; H04L-009/00

International Patent Class (Additional): G06F-009/302; G06F-013/20; G09C-001/00

File Segment: EPI; EngPI

```
Set     Items   Description
S1          7   (AU=((DROR I? OR DROR, I?) OR (GRESSEL C? OR GRESSEL, C?) -
                OR (MOSTOVOY M? OR MOSTOVOY, M?) OR (MOLCHANOV A? OR MOLCHANO-
                V, A?))) NOT (PY=(19990515:20020515) OR PY=(20020516:20060316-
                ))
```

? show files
File 348:EUROPEAN PATENTS 1978-2006/MAR
File 349:PCT FULLTEXT 1979-2006/UB=20060316,UT=20060309
(c) 2006 WIPO/Univentio

1/5/4 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00460387 **Image available**
IMPROVED APPARATUS & METHOD FOR MODULAR MULTIPLICATION & EXPONENTIATION BASED ON MONTGOMERY MULTIPLICATION
DISPOSITIF ET PROCEDE AMELIORES DE MULTIPLICATION MODULAIRE ET D'EXPONENTIATION BASES SUR UNE MULTIPLICATION DE MONTGOMERY
Patent Applicant/Assignee:
FORTRESS U & T LTD,
HADAD Isaac,
ARAZI Benjamin,
GRESSEL Carmi David,
DROR Itai,
Inventor(s):
HADAD Isaac,
ARAZI Benjamin,
GRESSEL Carmi David ,
DROR Itai
Patent and Priority Information (Country, Number, Date):
Patent: WO 9850851 A1 19981112
Application: WO 98IL148 19980329 (PCT/WO IL9800148)
Priority Application: IL 120776 19970504; IL 121311 19970714
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AT AU AZ BA BB BG BR BY CA CH CN CU CZ CZ DE DE DK DK EE EE ES
FI FI GB GE GH GM GW HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV
MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SK SL TJ TM TR TT UA
UG US UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM
AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA
GN ML MR NE SN TD TG
Main International Patent Class (v7): G06F-007/37
International Patent Class (v7): G06F-01:02; G06F-07:52
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 12119

English Abstract
This invention discloses a modular multiplication and exponentiation method and system including a serial-parallel arithmetic logic unit (ALU) including a single modular multiplying device (4 OPERAND MODULAR MULTIPLIER) having a single carry-save adder (410).

1/5/2 (Item 2 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00547666

Microcircuit for the implementation of RSA algorithm and ordinary and modular arithmetic, in particular exponentiation, with large operands.

Mikroschaltung fur die Implementation von RSA-Algorithmen und von gewohnlicher und modularer Arithmetik, insbesondere Exponentation, mit grossen Operanden.

Microcircuit pour l'implementation des algorithmes RSA et de l'arithmetique ordinaire et modulaire, particulierement l'exponentation, avec des grandes operandes

PATENT ASSIGNEE:
FORTRESS U&T (2000) Ltd., (1474730), P.O. Box 884, Beer-Sheva 84106, (US), (applicant designated states: DE;FR;GB;IT;NL)

INVENTOR:
Dariel, Eran Joseph, 188/21 Ahuza St.,, Raanana, (IL)
Gressel, Carmi David , Kibbutz Urim, D.N. Negev, (IL

LEGAL REPRESENTATIVE:
Joly, Jean-Jacques et al (39741), CABINET BEAU DE LOMENIE 55, rue d'Amsterdam, F-75008 Paris, (FR)

PATENT (CC, No, Kind, Date): EP 502782 A2 920909 (Basic)
EP 502782 A3 930414

APPLICATION (CC, No, Date): EP 92400554 920303;
PRIORITY (CC, No, Date): IL 97413 910304
DESIGNATED STATES: DE; FR; GB; IT; NL
INTERNATIONAL PATENT CLASS (V7): G06F-007/72;

CITED REFERENCES (EP A):
IEEE JOURNAL OF SOLID-STATE CIRCUITS vol. 23, no. 1, February 1988, NEW YORK US pages 204 - 207 LU 'A Programmable VLSI Architecture for Computing Multiplication and Polynomial Evaluation Modulo a Postive Integer'
Advances in Cryptology, CRYPTO '86, Pro- ceedings, pp277-301; Orton et al: 'VLSI implementation of pu blic-key encryption algorithms'
IEEE INTERNATIONAL SOLID STATE CIRCUITS CONFERENCE no. 31, 19 February 1988, NEW YORK US pages 140-141 - 332-333 , XP2122 HWANG ET AL 'THAM 11.2: A 3.1ns 32b CMOS Adder in Multiple Domino Logic'
Advances in Cryptology, EUROCRYPT '90, Denmark, Proceedings, pp230-244; Duss et al: 'A Cryptographic Library for the Motorola DSP56000'
Advances in Cryptology, CRYPTO '90, Pro- ceedings, pp619-624; Even: 'Systolic Modular Multiplication';

ABSTRACT EP 502782 A2
Microcircuit means for implementation of RSA encryption and decryption transformations are described, which consists of a plurality of units, to which external adders are attached, thereby incorporating the RSA function. (see image in original document)
ABSTRACT WORD COUNT: 37

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	920909	A2	Published application (A1with Search Report ;A2without Search Report)
Search Report:	930414	A3	Separate publication of the European or International search report
Examination:	931103	A2	Date of filing of request for examination: 930908
Examination:	970502	A2	Date of despatch of first examination report: 970313
Withdrawal:	980218	A2	Date on which the European patent application was deemed to be withdrawn: 970724

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	263
SPEC A	(English)	EPABF1	4842
Total word count - document A			5105
Total word count - document B			0
Total word count - documents A + B			5105